CCL331	CRYPTOGRAPHY LAB	CATEGORY	L	T	P	CREDITS
		PCC	0	0	4	2

Preamble: The aim of the Course is to give practical exposure on basic security attacks, encryption algorithms, and authentication techniques.

Prerequisite: Sound knowledge inApplied Cryptography and programming in C/ Java.

Course Outcomes: After the completion of the course the student will be able to

CO1	Use the different cipher techniques for securing information(**Cognitive Knowledge Level: Apply**)
CO2	Familiarize symmetric and asymmetric cryptography. (**Cognitive Knowledge Level: Apply**)
CO3	Demonstrate cryptographic principles and its applications. (**Cognitive Knowledge Level: Apply**)
CO4	Explain various approaches to Encryption techniques and message Authentication Codes. (**Cognitive Knowledge Level: Apply**)
CO5	Implement the algorithms DES,RSA(**Cognitive Knowledge Level: Apply**)
CO6	Write a program using linked lists to simulate Memory Allocation and Garbage Collection(**Cognitive Knowledge Level: Apply**)

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	✔	✔	✔	✔		✔						✔
CO2	✔	✔	✔	✔								✔
CO3	✔	✔	✔	✔								✔
CO4	✔	✔	✔	✔								✔
CO5	✔	✔	✔									✔
CO6	✔	✔	✔									✔

Abstract POs defined by National Board of Accreditation			
PO#	Broad PO	PO#	Broad PO
PO1	Engineering Knowledge	PO7	Environment and Sustainability
PO2	Problem Analysis	PO8	Ethics
PO3	Design/Development of solutions	PO9	Individual and teamwork
PO4	Conduct investigations of complex problems	PO10	Communication
PO5	Modern tool usage	PO11	Project Management and Finance
PO6	The Engineer and Society	PO12	Lifelong learning

Assessment Pattern

Bloom's Category	Continuous Assessment Test(Internal Exam) (%)	End Semester Examination (%)
Remember	20	20
Understand	20	20
Apply	60	60
Analyze		
Evaluate		
Create		

Mark Distribution

Total Marks	CIE Marks	ESE Marks	ESE Duration
150	75	75	3hours

Continuous Internal Evaluation Pattern:

Attendance:15 marks
Continuous Evaluation in Lab :30 marks
Continuous Assessment Test   : 15 marks
Viva-voce:15 marks

Internal Examination Pattern:

The marks will be distributed as Algorithm 30 marks, Program20 marks, Output 20 marks and Viva 30 marks. Total 100 marks which will be converted out of 75 while calculating Internal Evaluation marks.

End Semester Examination Pattern:

The marks will be distributed as Algorithm 30 marks, Program 20 marks, Output 20 marks and Viva 30 marks. Total 100 marks will be converted out of 75 for End Semester Examination.

Operating System to Use in Lab :Linux

Compiler/Software to Use in Lab:gcc
Programming Language to Use in Lab : Ansi C and Java

Fair Lab Record:

All Students attending the Lab should have a Fair Record. The fair record should be produced in the University Lab Examination. Every experiment conducted in the lab should be noted in the fair record. For every experiment in the fair record the right hand page should contain Experiment Heading, Experiment Number, Date of Experiment, Aim of Experiment, Data Structure used and the operations performed on them, Details of Experiment including algorithm and Result of Experiment. The left hand page should contain a print out of the code used for the experiment and sample output obtained for a set of input.

Syllabus

*mandatory

1. Represent a string (char pointer) with a value "Hello world". The program should XOR each character in this string with 0 and displays the result.*

2. Represent string (char pointer) with a value "Hello world" The program should AND or and XOR each character in this string with 127and display the result.

3. Perform encryption and decryption using the following algorithms*

   a. Ceaser cipher b. Substitution cipher c. Hill Cipher

4. Implementation of Encryption and Decryption using DES*

5. Implementation of RSA Encryption Algorithm

6. Implementation of Hash Functions*

7. Implementation of Blowfish algorithm logic*

8. Implement the Diffie-Hellman Key Exchange mechanism

9. Implement RC4 logic using Java*

10. Encrypt the text "Hello world" using Blowfish.

11. Implement the SIGNATURE SCHEME –Digital Signature Standard*

PRACTICE QUESTIONS

1. Write a C program that contains a string (char pointer) with a value"Helloworld". The program should XOR each character in this string with 0 and displays the result.

2. Write a C program that contains a string (char pointer) with a value „Hello world". The program should AND or and XOR each character in this string with 127 and display the result.

3. Write a Java program to perform encryption and decryption using the following algorithms
       a.Caeser cipher   b. Substitution cipher c.Hill Cipher

4. Write a C/JAVA program to implement DES Encryption and Decryption

5.   Write a C/JAVA program to implement RSA Encryption Algorithm

6. Write a C/JAVA program to implementation of Hash Functions.

7. Write a C/JAVA program to implement the Blowfish algorithm logic.

8. Write the RC4 logic in Java Using Java cryptography; encrypt the text Hello world using Blowfish. Create your own key using Java key tool.

9. Write a C/JAVA program to implement the Diffie-Hellman Key Exchange mechanism

10. Implement the SIGNATURE SCHEME –Digital Signature Standard